AO 106 (Rev. 04/10) Application for a Search Warrant

Authorized and approved:

FILED
NOV 20 2020
CARMELITA REEDER SHIN
CLERK, U.S. DISTRICT COURT
BY [signature] DEPUTY

UNITED STATES DISTRICT COURT

for the

Western District of Oklahoma

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
A Dell Model P58F Laptop with Barcode Number 38533378754 and Service Tag (S/N) HP9S1C2 Currently Located in Secure Evidence Storage at the HSI Office in Oklahoma City, OK

Case No. M-20-575 -P

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A (Device 2)

located in the Western District of Oklahoma, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. § 841(a)(1)	Drug Trafficking
21 U.S.C. § 846	Drug Conspiracy

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

[signature]
Applicant's signature

RYDER BURPO, Special Agent, HSI
Printed name and title

Sworn to before me and signed in my presence.

Date: 11/20/20

[signature]
Judge's signature

City and state: Oklahoma City, Oklahoma

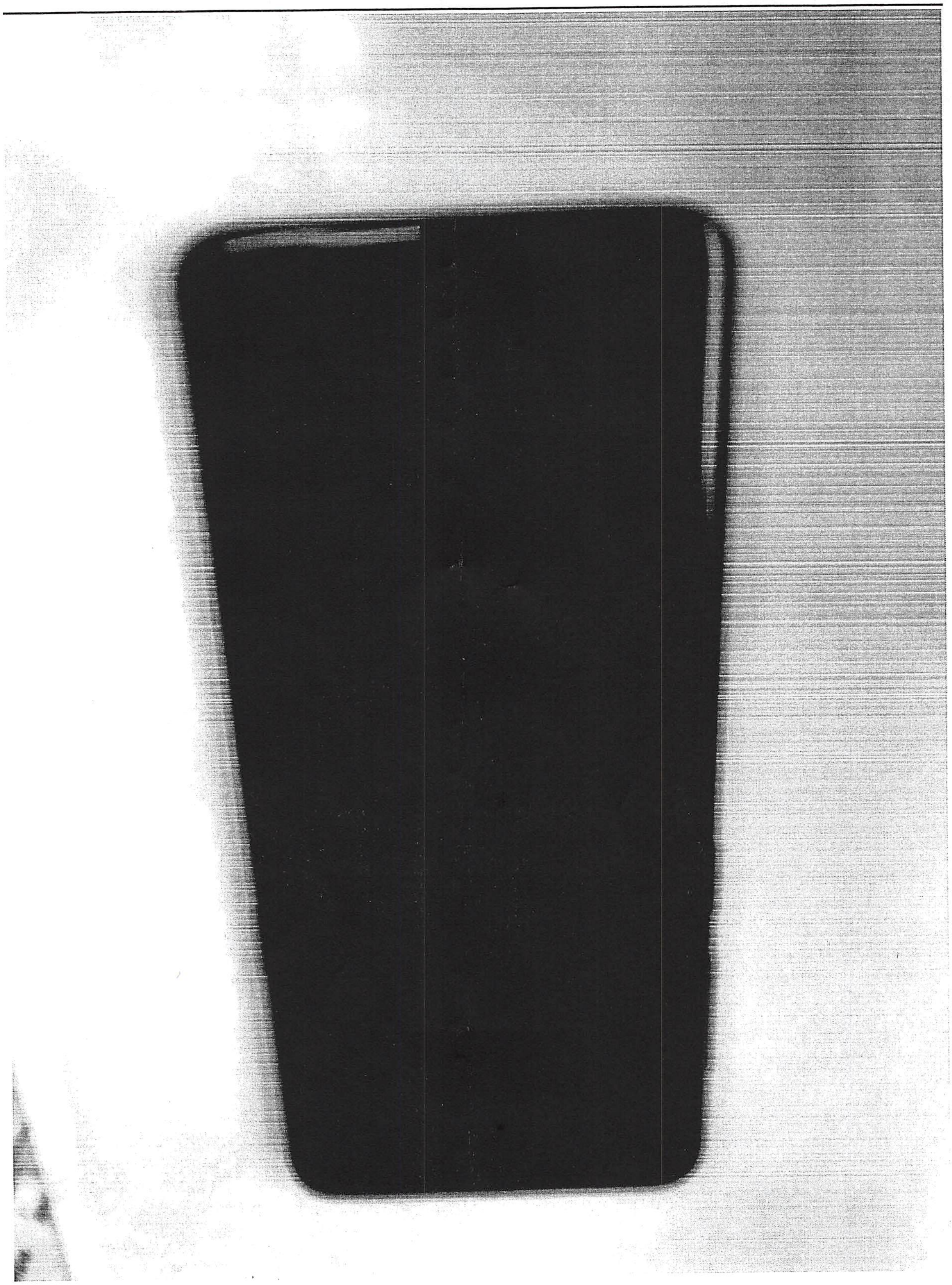
GARY M. PURCELL, U.S. Magistrate Judge
Printed name and title

AUSA: Matthew Anderson

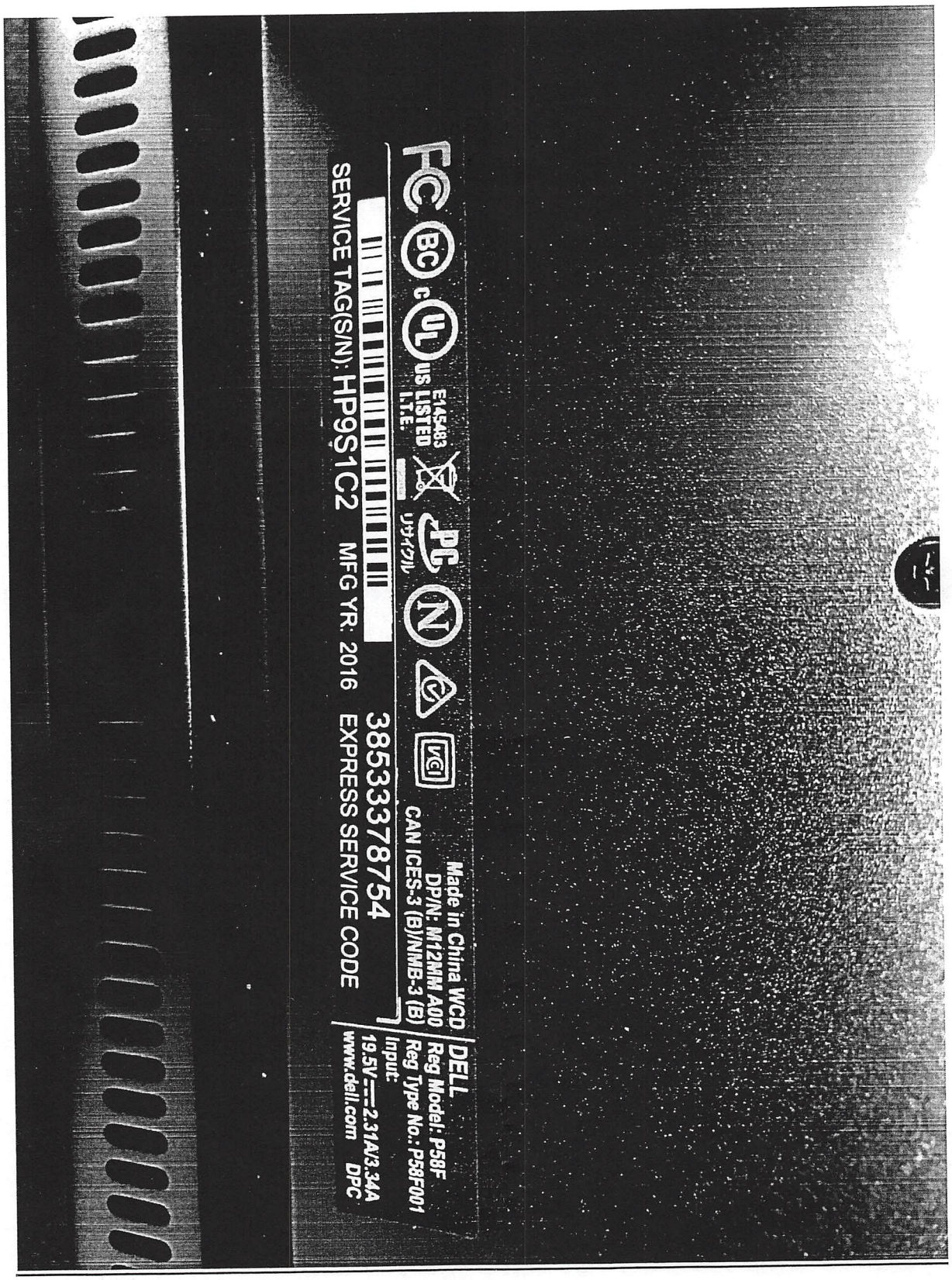
ATTACHMENT "A"
Items to be searched

Device 1. Samsung SM-G960U with IMEI 359943091231694

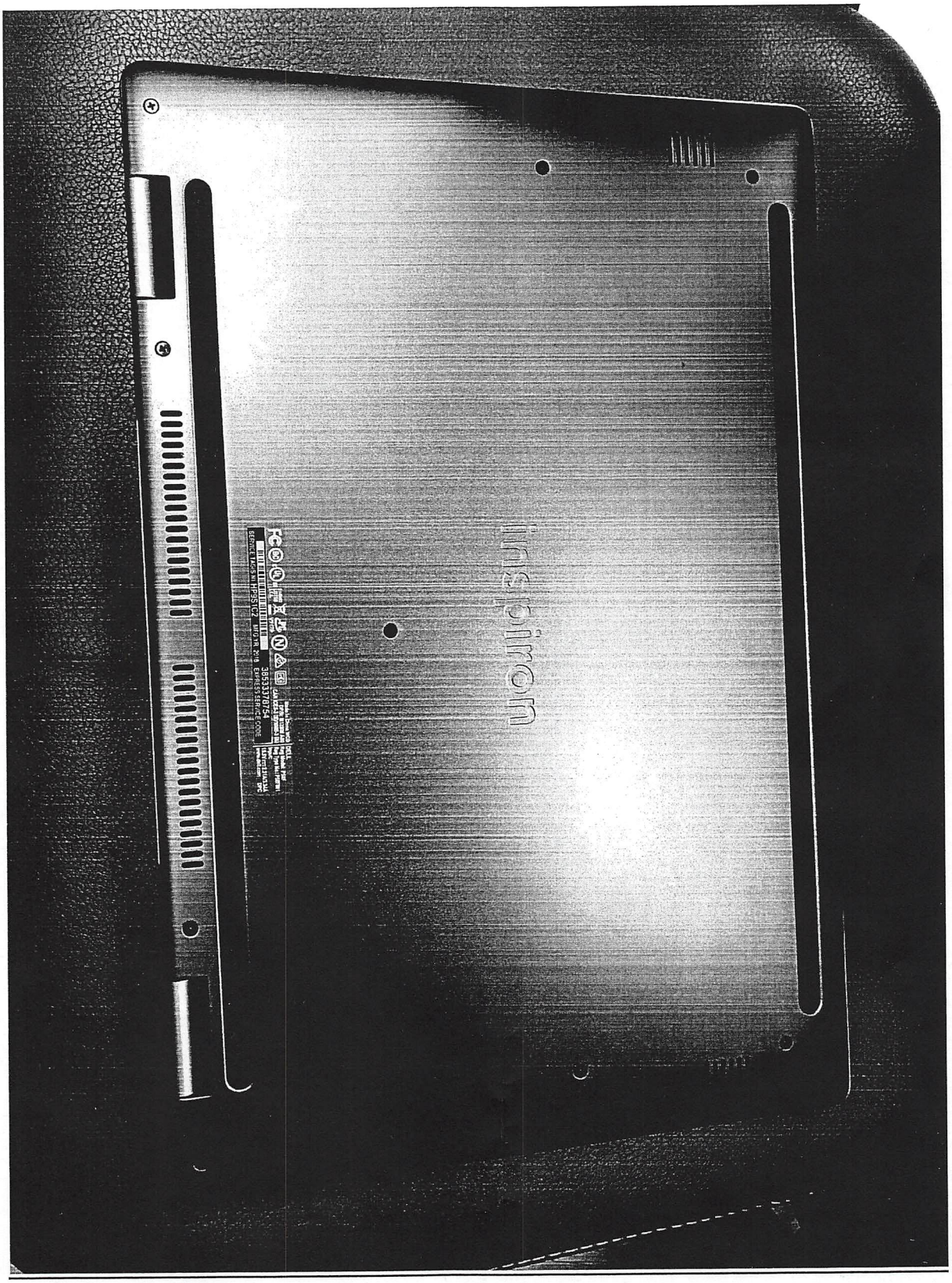
RB



Device 2. Dell Model P58F Laptop with Barcode Number 38533378754 and Service Tag(S/N) HP9S1C2


DELL
Reg Model: P58F
Reg Type No.: P58F001
Input:
19.5V ⎓ 2.31A/3.34A
www.dell.com DPC
Made in China WCD
DP/N: M12MM A00
CAN ICES-3 (B)/NMB-3 (B)
E145483
US LISTED
I.T.E.
リサイクル
38533378754
SERVICE TAG(S/N): HP9S1C2 MFG YR: 2016 EXPRESS SERVICE CODE

AB



RB

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of 21 U.S.C. §§ 841(a)(1), 846 involving STULL including information pertaining to the following matters:

a. Lists of customers and related identifying information;

b. Types, amounts, and prices of controlled substances as well as dates, places, and amounts of specific transactions;

c. Any information related to sources of controlled substances (including names, addresses, phone numbers, emails, notes or any other identifying information);

d. Any information concerning the transportation or shipment of controlled substances;

e. Communications regarding controlled substance offenses;

f. All bank records, checks, credit card bills, account information, and other financial records;

g. Evidence related to the possession, use, storage, or purchase of any vehicles, vessels, or other items that could be used as a means of transporting controlled substances;

h. Evidence, including geolocation records, related to locations used as meeting places, places used to store proceeds, instrumentalities, controlled

KB

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF OKLAHOMA

IN THE MATTER OF THE SEARCH OF A SAMSUNG SM-G960U PHONE WITH IMEI 359943091231694 AND A DELL MODEL P58F LAPTOP WITH BARCODE NUMBER 38533378754 AND SERVICE TAG (S/N) HP9S1C2 CURRENTLY LOCATED IN SECURE EVIDENCE STORAGE AT THE HSI OFFICE IN OKLAHOMA CITY, OK	**Case No.** _____

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Ryder Burpo, being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am an investigative or law enforcement officer within the meaning of 18 U.S.C. § 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in 18 U.S.C. § 2516. I have bene employed as a Special Agent of the U.S. Department of Homeland Security, Homeland Security Investigations (HSI) since June 2019. I am presently assigned to the HSI office in Oklahoma City, Oklahoma (hereinafter referred to as HSI

Oklahoma City). As a Special Agent, I am authorized to conduct criminal investigations of violations of the United States and to execute warrants issued under the authority of the United States.

3. I have received approximately 28 weeks of specialized training at the Federal Law Enforcement Training Center in the enforcement of federal laws. Before my current position, I was employed by the Law Enforcement Support Center as a Law Enforcement Specialist for two and a half years. Prior to that I served as an Unmanned Aerial Vehicle operator in the United States Army.

4. I have arrested, interviewed, and debriefed individuals who have been involved and have personal knowledge of importing, transporting, and concealing controlled substances, as well as the amassing, spending, converting, transporting, distributing, laundering and concealing of proceeds from controlled substance trafficking and smuggling. I have testified in judicial proceedings concerning the prosecution for violations of laws related to the unlawful possession of firearms and smuggling and trafficking of contraband, including controlled substances. I have been the affiant of search warrants, including warrants authorizing the search of electronic devices.

5. Based on my training and experience, I know that individuals who are involved in criminal organizations maintain books, records, receipts, notes, ledgers, and other papers relating to their clients and associates. Furthermore, based on my training and experience, I know that these individuals often utilize phones, computers, emails, text messages, and other computer-facilitated communication software to communicate and maintain contact with their clients and associates.

6. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

7. Based on the facts set forth in this affidavit, I believe that there is probable cause that Wallace Bradley STULL violated Title 21, United States Code, Sections 841(a)(1) and 846. Specifically, there is probable cause to believe that STULL possessed with the intent to distribute marijuana and conspired with others, known and unknown, to possess with the intent to distribute marijuana. There is also probable cause to believe that the information described in Attachment B will constitute evidence of these criminal violations and will lead to the identification of individuals who are engaged in the commission of these offenses.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

8. This affidavit is made in support of an application for a warrant to search a Samsung SM-G960U with IMEI 359943091231694, hereinafter "Device 1", and a Dell Model P58F Laptop with Barcode Number 38533378754 and Service Tag (S/N) HP9S1C2, hereinafter "Device 2." Collectively, Device 1 and Device 2 will be referred to as the "Devices." The Devices are currently in secure evidence storage at HSI Oklahoma City, located at 3625 NW 56th St, Oklahoma City, OK.

9. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

FACTUAL BACKGROUND

10. On October 23, 2020, HSI Oklahoma City received information from HSI Medford, Oregon about a suspicious shipment being shipped to the Old Dominion freight terminal in Oklahoma City. The shipping manifest listed the shipment as two pallets of synthetic gloves with a weight of 2,675 pounds. The two-pallet shipment was being shipped by STULL at Pacific Supply in Eagle Point, Oregon to "Mike" at Sun Gloves, 13505 Railway Drive, #G, Oklahoma City, OK 73114.

11. On November 2, 2020, law enforcement confirmed the shipment was at the Old Dominion freight yard at 1400 S. Skyline Drive in Oklahoma City. The shipment consisted of two pallets, each pallet consisting of approximately 36 cardboard boxes shrink-wrapped together. I arranged for an Oklahoma City Police Department K-9 to conduct a free-air sniff of the shipment. The free air sniff resulted in positive indications for the odor of controlled substances from boxes on both pallets. A state search warrant for the shipment was subsequently obtained.

12. At approximately 10:00 a.m., HSI Oklahoma City, DEA Oklahoma City, and Oklahoma City Police Department personnel executed the search warrant by cutting the shrink wrap around one of the pallets and opened each of the 36 boxes. Three boxes contained only vacuum sealed bags of marijuana. Seventeen boxes contained vacuum sealed bags of marijuana along with boxes of latex gloves. The remaining sixteen boxes contained latex gloves. Agents looked in only one box from the second pallet that contained only vacuum sealed bags of marijuana.

13. On November 3, 2020, HSI Oklahoma City and DEA Oklahoma City conducted a controlled delivery of the marijuana from Old Dominion to 13505 Railway Drive Suite G, Oklahoma City, Oklahoma 73114. An older white male was observed by law enforcement receiving the two pallets containing marijuana and signing for the shipment. This older white male was subsequently identified as STULL.

14. Approximately thirty minutes after the suspected marijuana was delivered to the Railway Drive warehouse, agents observed a blue Ford Escape arrive at the warehouse. Agents observed a younger white male briefly enter the door to Suite G of the warehouse and speak with STULL. Agents then observed both males depart the warehouse in separate vehicles and travel in tandem away from the business. STULL was observed departing the location in a white Ford F250 pickup bearing Oklahoma tag EFC 897. Registration information on the F250 returned to Conner STEVENSON, 2811 Drakestone Avenue in Oklahoma City, Oklahoma. The younger white male was observed departing in blue Ford Escape and later identified as STEVENSON.

15. Several minutes later, Agents observed a blue Ford Escape in the driveway of 2811 Drakestone Avenue. Surveillance agents observed the white F250 appear to make several "heat runs" after departing the Railway Drive warehouse that appeared designed to determine whether he was being followed. Law enforcement eventually stopped the F250 a short distance away from the Drakestone address and the driver was detained. The older white male driver of the F250 was identified by California Driver's License as STULL.

16. DEA Oklahoma City seized the Ford F250 for purposes of administrative forfeiture based on its use to facilitate the distribution of controlled substances and based on its purchase through the use of proceeds from illegal acts. Prior to its seizure, law enforcement inventoried its contents. During the inventory of the vehicle, law enforcement discovered and seized $2,400 of U.S. currency and receipts for a hotel in Oregon just prior to the shipment of marijuana, a ledger containing prices and names of marijuana strains, the names of which were the same as the vacuum sealed bags that were seized. Law enforcement also discovered the Devices inside the Ford F250. Later that day, law enforcement executed a search warrant at the Railway Drive warehouse and ultimately recovered 328 pounds of marijuana.

17. Based on my training and experience, I believe STULL was knowingly receiving marijuana from Oregon at 13505 Railway Drive, Oklahoma City, Oklahoma according to the bill of lading, the attempted heat runs after he left 13505 Railway Drive, and the fact the marijuana was concealed within boxes with latex gloves. Given the amount of marijuana, it is my belief that STULL intended to distribute the marijuana.

18. The Devices are currently located in secure evidence storage at HSI Oklahoma City, located at 3625 NW 56th St., Oklahoma City, OK. In my training and experience, I know that the Devices have been stored in a manner in which its contents are (to the extent material to this investigation) in substantially the same state as they were when the Devices first came into the possession of HSI.

19. Based on my training, experience, and research, I know that Device 1 has the capability to serve as a wireless telephone, digital camera, portable media player, GPS

navigation device, and PDA. In my training and experience, examining data stored on a device of this type can uncover, among other things, evidence that reveals or suggests who possessed or used Device 1.

20. From my training and experience, I know that drug trafficking is a conspiratorial crime. Individuals who possess controlled substances do so with the assistance of others. Drug traffickers often use their cell phones to communicate with other members of the drug trafficking organization. Records of these communications, and the contact information of other conspirators are often saved in the phone.

21. An examination can reveal the approximate location of the Device 1 and the user by associating a specific date and time with: historical GPS data, historical cell-site data, and logs of Wi-Fi networks. Additionally, an examination can reveal the Devices' unique identifiers (phone number, IMEI, IMSI, etc.). These unique identifiers can be used to compel material records from the cell phone service provider such as call logs, billing information, and historical cell-site data.

22. Based on my training, experience, and research, I know that Device 2 has the capability to serve as a wireless communication device, portable media player, and PDA. In my training and experience, examining data stored on a device of this type can uncover, among other things, evidence that reveals or suggests who possessed or used Device 2.

23. From my training and experience, I know that drug trafficking is a conspiratorial crime. Individuals who possess controlled substances do so with the assistance of others. Drug traffickers often use their laptops to communicate with other

members of the drug trafficking organization. Records of these communications, and the contact information of other conspirators are often saved in the laptop.

24. An examination can reveal the approximate location of the Device 2 and the user by associating a specific date and time with logs of Wi-Fi networks. Additionally, an examination can reveal the Devices' unique identifiers (MAC address, CPU Serial number, etc.). These unique identifiers can be used to compel material records from the internet service provider such as Internet Service provider logs, and billing information.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

25. I know based upon my training and experience that computer hardware, software, documentation, passwords, and data security devices may be important to a criminal investigation in two distinct and important respects: (1) the objects themselves may be instrumentalities, fruits, or evidence of crime, and/or (2) the objects may have been used to collect and store information about crimes (in the form of electronic data). Rule 41 of the Federal Rules of Criminal Procedure permits the government to search and seize computer hardware, software, documentation, passwords, and data security devices, which are (1) instrumentalities, fruits, or evidence of crime; or (2) storage devices for information about crime.

26. Based upon my knowledge, training and experience, and consultations with computer specialists, I know that the search and seizure of information from computers often requires agents to seize most or all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other

controlled environment. This is true because of the volume of evidence contained on computer storage devices and the technical requirements needed to properly search those devices.

27. Based upon my knowledge, training and experience, and consultation with computer specialists, I know that searching computerized information for evidence or instrumentalities of crime commonly requires agents to seize most or all of a computer system's input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. This is true because the peripheral devices which allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output (or "I/O") devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as, all related instruction manuals or other documentation and data security devices.

28. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

29. There is probable cause to believe that things that were once stored on the Devices may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from the operating system or application operation, file system data structures, and virtual memory

"swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet director or "cache."

30. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining the forensic evidence in its proper context, be able to

draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on a computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

31. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Devices to human inspection in order to determine whether it is evidence described by the warrant.

32. *Manner of execution.* Because this warrant seeks only permission to examine the devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit

there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

33. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

RYDER BURPO
Special Agent, HSI

Subscribed to and sworn before me on November 20, 2020.

GARY M. PURCELL
United States Magistrate Judge

ATTACHMENT "A"
Items to be searched

Device 1. Samsung SM-G960U with IMEI 359943091231694

RB

RB

Device 2. Dell Model P58F Laptop with Barcode Number 38533378754 and Service Tag(S/N) HP9S1C2

RB


E145483
US LISTED
I.T.E.
Made in China WCD
DP/N: M12MM A00
CAN ICES-3 (B)/NMB-3 (B)
DELL
Reg Model: P58F
Reg Type No.: P58F001
Input:
19.5V ⎓ 2.31A/3.34A
www.dell.com DPC
SERVICE TAG(S/N): HP9S1C2 MFG YR: 2016 EXPRESS SERVICE CODE
38533378754

RB

12B

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of 21 U.S.C. §§ 841(a)(1), 846 involving STULL including information pertaining to the following matters:

a. Lists of customers and related identifying information;

b. Types, amounts, and prices of controlled substances as well as dates, places, and amounts of specific transactions;

c. Any information related to sources of controlled substances (including names, addresses, phone numbers, emails, notes or any other identifying information);

d. Any information concerning the transportation or shipment of controlled substances;

e. Communications regarding controlled substance offenses;

f. All bank records, checks, credit card bills, account information, and other financial records;

g. Evidence related to the possession, use, storage, or purchase of any vehicles, vessels, or other items that could be used as a means of transporting controlled substances;

h. Evidence, including geolocation records, related to locations used as meeting places, places used to store proceeds, instrumentalities, controlled

RB

substances, firearms possessed or used in the furtherance of drug trafficking, or other contraband;

i. Phone call records (incoming, outgoing, missed calls), voicemail, text messages (mms/sms/picture/video/etc.), emails, video chats, direct messaging, encoded messaging, mobile applications, and all other forms of communication that could be utilized to plan and discuss the transportation, packaging, distribution, sale, or concealment of controlled substances or drug proceeds;

j. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames, passwords, documents, and browsing history;

k. Any digital data or material including video, audio, and still photography, lists, notes, and other text data relating to the distribution of controlled substances; and

l. Call history, contact name and numbers, voice and text messages, emails, pictures, videos, and/or other electronic data relating to drug activity.

RB